

Update on Encryption algorithm Rocca-S draft-nakano-rocca-s

Yuto Nakano, Kazuhide Fukushima, Takanori Isobe

CFRG@IETF116

Security evaluation by 3rd party

- Rocca-S has been confirmed to be secure against following attacks

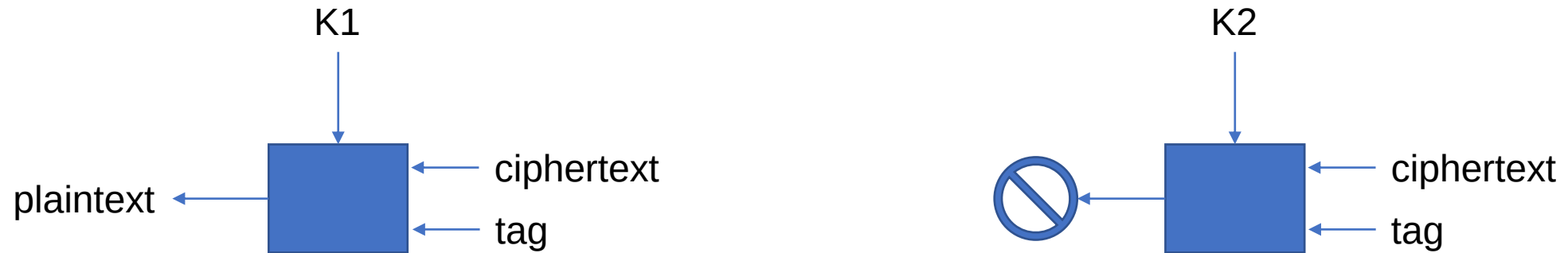
	Indian Institute of Technology Madras(*)	University of Rennes 1 (**)
Differential Attack	✓	✓
Linear Attack	✓	✓
Forgery Attack	✓	✓
Integral Attack		✓
State-recovery Attack		✓

(*) : Prof. Santanu Sarkar

(**): Prof. Patrick Derbez

New security claim

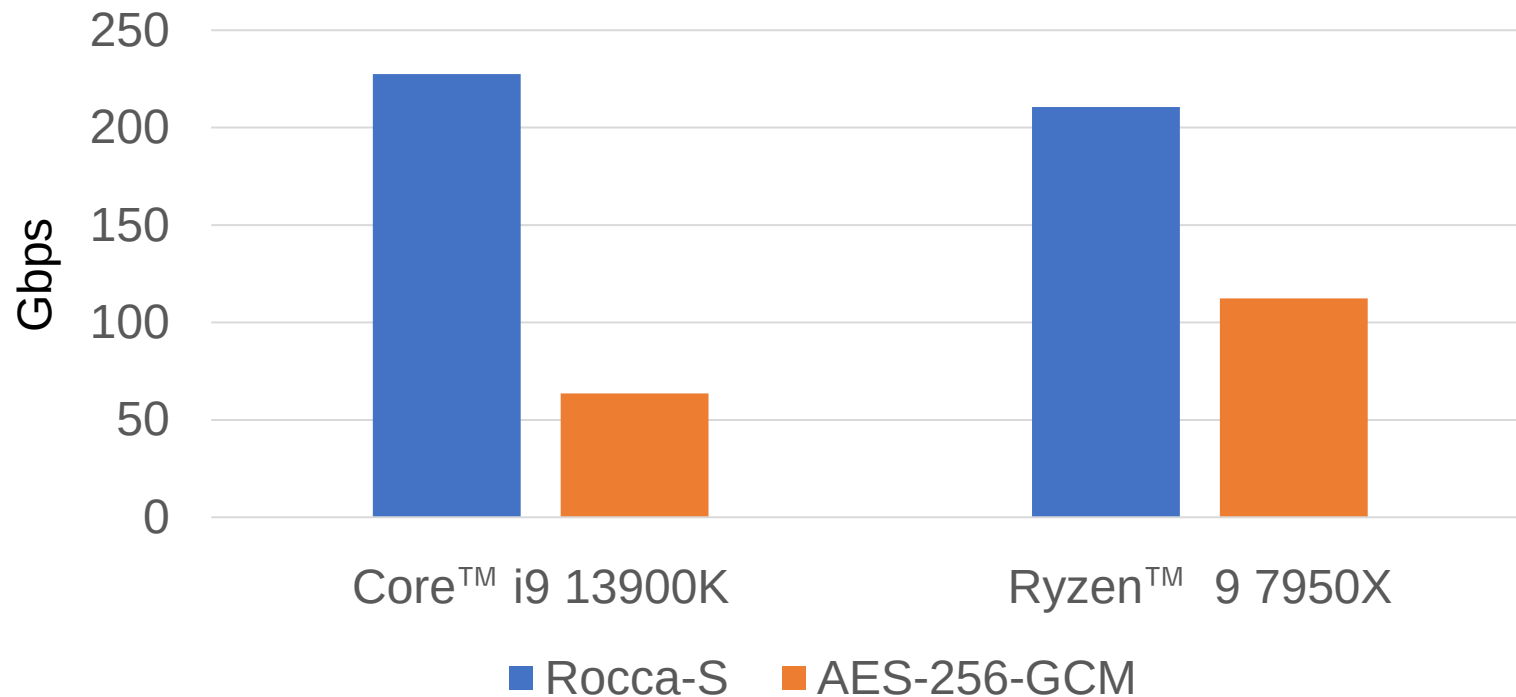
- Key-committing security
 - Ciphertext can only be decrypted with *the same key* which is used for the encryption



- Rocca-S provides 128-bit key-committing security

Update on performance evaluation

- Evaluation results with “openssl -speed” on Core™ i9 13900K and Ryzen™ 9 7950X



Opensource

Reference implementation is available at
<https://github.com/yt-nakano/rocca-s>

Free to use with your application!!